UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/649,169	08/27/2003	Leedor Agam	2808/53	4740

7590 03/07/2007

Dr. Mark Friedman Ltd.
c/o Polkinghorn
9003 Florin Way
Upper Markboro, MD 20772

EXAMINER	
SHAN, APRIL YING	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS.	03/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/649,169	AGAM ET AL.	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 1**, "said host" is recited. Since no host is ever recited in the claim, "said host" lacks of antecedent basis. Additionally, "the power supply" is recited in claim 1. Since no power supply is ever recited in the claim, "the power supply" lacks of antecedent basis.

As per **claim 2**, "said one-time password" is recited. Since no one-time password ever recited in the claim, "said one-time password" lacks of antecedent basis.

As per **claim 5**, "the password" is recited. In light of Applicant's specification, there are password and one-time password. Which password the Applicant is referring to? Additionally, "the password" lacks of antecedent basis. Further, "the displayed valued" lacks of antecedent basis. Also, in light of Applicant's specification on page 8, the Applicant discloses "that provided value doesn't necessarily equal the expected value, but should "correspond" to the

expected value. So, what value the Applicant is referring to? Furthermore, "a host" is the same as the "said host" recited in claim 1?

As per **claim 6**, "a power supply" is recited. Is it the same as "the power supply" recited in claim 1?

As per **claim 7**, "the power" is recited. It lacks of antecedent basis.

As per **claim 8**, "said host" is recited. It lacks of antecedent basis. Additionally, "said encrypted one-time value" lacks of antecedent basis.

As per **claim 9**, "said one-time password" lacks of antecedent basis.

As per **claim 12**, "the real time" lacks of antecedent basis. Additionally, "the value of a counter" lacks of antecedent basis.

As per **claim 13**, "the password" is recited. In light of Applicant's specification, there are password and one-time password. Which password the Applicant is referring to? Additionally, "the password" lacks of antecedent basis. Further, "the displayed valued" lacks of antecedent basis. Also, in light of Applicant's specification on page 8, the Applicant discloses "that provided value doesn't necessarily equal the expected value, but should "correspond" to the expected value. So, what value the Applicant is referring to? Furthermore, "a host" is the same as the "said host" recited in claim 8?

As per **claim 16**, "said host" is recited. It lacks of antecedent basis. Additionally, "the power supply" lacks of antecedent basis.

As per **claim 17**, "the password" is recited. In light of Applicant's specification, there are password and one-time password. Which password the

Applicant is referring to? Additionally, "the password" lacks of antecedent basis. Further, "the displayed valued" lacks of antecedent basis. Also, in light of Applicant's specification on page 8, the Applicant discloses "that provided value doesn't necessarily equal the expected value, but should "correspond" to the expected value. So, what value the Applicant is referring to?

As per **claim 18**, "the power" lacks of antecedent basis.

As per **claim 19**, "said value" is recited. Which value the Applicant is referring to, a first one-time value from step (a) or the one time value after the performing public-key functionality from step (b)?

As per **claim 20**, "said one-time value" is recited. However, in claim 19, there are two one-time values. Which one is the Applicant referring to?

As per **claim 21**, "the encrypted value" and "said host" are lack of antecedent basis.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al. (U.S. Pub. No. 20050015588).

As per **claim 1**, Lin et al. discloses a security token, comprising:

a one-time password mechanism, for rendering one-time password functionality (e.g. paragraph [0034]);

a public-key mechanism, for rendering public-key functionality with respect to said one-time password functionality (e.g. paragraphs [0033]- [0034]);

and communication means for connecting said security token to said host and ("the token includes an interface for coupling to a computer" – e.g. abstract., paragraph [0028]. Please note an interface corresponds to Applicant's communication means and a computer corresponds to Applicant's host).

Lin et al. does not expressly disclose the communication means for providing to said security token the power supply required for operating at least said public-key mechanism. However, Lin et al. discloses in paragraph [0028], "preferably, the interface 26 is provided in a known Universal Serial Bus (USB) configuration for coupling to a

known USB port 28 of the computer 30 via a USB data cable 32". To a person with ordinary skill in the art, USB configuration provides power to the security token.

It would have been obvious that the interface of Lin et al. provides the security token the power supply required for operating at least said public-key mechanism.

The motivation of doing so would have been USB is a serial bus standard to interface device and it is well known that USB provides power to the security token.

As per **claim 2**, Lin et al. discloses a token as applied above in claim 1. Lin et al. further discloses comprising a display, for displaying at least said one-time password (e.g. paragraph [0024]).

As per **claim 3**, Lin et al. discloses a token as applied above in claim 1. Lin et al. further discloses comprising a smartcard chip, for secure storage of keys and for rendering security-related functionality (e.g. paragraph [0024]).

As per **claim 4**, Lin et al. discloses a token as applied above in claim 1. Lin et al. further discloses wherein said one-time password mechanism comprise means for generating a one-time value, said means selected from a group comprising: a real-time clock, and a counter (e.g. paragraph [0033]).

As per **claim 5**, Lin et al. discloses a token as applied above in claim 1. Lin et al. further discloses wherein said communication means is selected from a group

comprising: a display for displaying the password and thereafter manually providing the displayed value to a host, means for connecting said security token to said host via a wired connection, and means for connecting said security token to said host via a wireless connection (e.g. paragraph [0028]).

As per **claim 6**, Lin et al. discloses a token as applied above in claim 5. Lin et al. further discloses wherein said wired communication means further comprise means for providing a power supply to said security token (Please see rationale in rejecting claim 1 above).

As per **claim 7**, Lin et al. discloses a token as applied above in claim 5. Lin et al. does not expressly discloses comprising a chargeable power source, to be charged by the power supplied via said communication means, for providing the power for operating said security token while not connected to said host. However, examiner takes official notice that it is common knowledge and well known in the art. It would have been obvious to a person with ordinary skill in the art to incorporate a chargeable power source, to be charged by the power supplied via said communication means, for providing the power for operating said security token while not connected to said host into Lin et al.'s token. The motivation of doing so would have been to assure that the token is well charged.

As per **claim 8**, Lin et al. discloses a one-time password security token, for securely providing a one-time value to a host system, said one-time password security token comprising: means for generating said one-time value (please see rationale in rejecting claim 1 above); a public-key infrastructure mechanism, for performing public-key functionality with respect to said one-time value (please see rationale in rejecting claim 1 above); and communication means for connecting said security token with said host and for providing said encrypted one-time value to said host (e.g. paragraph [0028]).

As per **claim 9**, Lin et al. discloses a token as applied above in claim 8. Lin et al. further discloses wherein said public-key functionality with respect to said one-time value is selected from a group comprising: encrypting said one-time value by said public-key functionality, and digitally signing said one-time password (e.g. paragraphs [0033]-[0034]).

As per **claim 10**, Lin et al. discloses a token as applied above in claim 8. Lin et al. further discloses comprising a display, for displaying at least the encrypted one-time value (e.g. paragraphs [0015], [0024] and [0033]-[0034]).

As per **claims 11 and 14**, Lin et al. discloses a token as applied above in claim 8. Lin et al. further discloses comprising a smartcard chip, for rendering security-related functionality (please see rationale in rejecting claim 3 above) and wherein said wired

communication means further comprise means for providing a power supply to said security token (e.g. paragraph [0028]).

As per **claim 12**, Lin et al. discloses a token as applied above in claim 8. Lin et al. further discloses wherein said one-time value is selected from a group comprising: the real-time, the value of a counter, and a group of random numbers (e.g. paragraphs [0015] and [0033]).

As per **claim 13**, Lin et al. discloses a token as applied above in claim 13. Lin et al. further discloses wherein said communication means is selected from a group comprising: a display for displaying the password and thereafter manually providing the displayed value to said host, wired communication means with said host, wireless communication means with said host (e.g. paragraphs [0024] and [0028]).

As per **claim 15**, Lin et al. discloses a token as applied above in claim 8. Lin et al. further discloses a chargeable power source, to be charged by the power supplied by said communication means, for providing the power for operating said security token while not connected to said host (please see above rationale in rejecting claim 7 above).

As per **claim 16**, Lin et al. discloses a security system comprising: at least one security token comprising: a one-time password mechanism, for rendering one-time

password functionality (please see rationale in rejecting claim 1 above); a public-key mechanism, for rendering public-key functionality with respect to said one-time password functionality (please see rationale in rejecting claim 1 above); and communication means for connecting said security token to said host and for providing to said security token the power supply required for operating at least said public-key mechanism (please see above rationale in rejecting claim 1 above); a host system, comprising communication means, corresponding to the communication means of said at least one security token, for communicating with said at least one security token (e.g. paragraph [0028]) and for providing to said token the power supply required for operating at least the public-key mechanism of said security token (Please see rationale in rejecting claim 1 above).

Lin et al. further discloses in the abstract that "A token device that generates and displays one-time passwords and couples to a computer for inputting or receiving data for generating and outputting one-time passwords and performing other functions is provided" and Lin et al. Therefore, it would have been obvious to a person with ordinary skill in the art at the time of the invention that a host system can have a one-time password mechanism, corresponding to the one-time password mechanism of said at least one security token, for rendering one-time password functionality; a public-key mechanism, corresponding to the public-key mechanism of said at least one security token, for rendering public-key functionality.

The motivation of doing so would have been in order for a host system to "inputting or receiving data for generating and outputting one-time passwords and performing other functions is provided", as taught by the abstract of Lin et al.

As per **claim 17**, Lin et al. discloses a system as applied above in claim 16. Lin et al. further discloses wherein said communication means is selected from a group comprising: a display embedded within each of said at least one security token, for displaying the password and thereafter manually providing the displayed value to said host, wired communication means through which said at least one security token can be provided with the power supply required for performing public-key operations (e.g. paragraph [0028]).

As per **claim 18**, Lin et al. discloses a system as applied above in claim 16. Lin et al. further discloses wherein each of said at least one security token further comprising chargeable power source, to be charged via the power supply provided by said communication means, for providing the power for operating said at least one processor while not connected to said host, thereby enabling to operate said security token without external power supply (Please see above rationale in rejecting claim 7 above).

As per **claim 19**, Lin et al. discloses a method for authenticating a client by a host system, said method comprising: at said client side: (a) generating a first one-time

value (see rationale in rejecting claim 1 above); (b) performing public-key functionality with respect to said one-time value (see rationale in rejecting claim 1 above); (c) providing said value to said host system (e.g. paragraph [0028]); at said host system side: (d) performing public-key functionality which corresponds to the public key functionality performed at step (b) with the provided value (Please see rationale in rejecting claim 16 above); (e) generating a second one-time value in substantially the same manner as said first one-time value is generated (Please see rationale in rejecting claim 16 above); authenticating said client by the correspondence of said second value to said first value (e.g. paragraph [0034]).

As per **claim 20**, Lin et al. discloses a method as applied above in claim 19. Lin et al. further discloses wherein said public-key functionality with respect to said one-time value is selected from a group comprising: encrypting said one-time value, and digitally signing said one-time value (e.g. paragraphs [0015], [0033]-[0034])

As per **claim 21**, Lin et al. discloses a method as applied above in claim 19. Lin et al. further discloses wherein said client is a security token (e.g. abstract).

As per **claim 22**, Lin et al. discloses a method as applied above in claim 19. Lin et al. further discloses wherein providing the encrypted value to said host is carried out by a member of a group comprising: displaying said encrypted value at the client side and thereafter manually providing the displayed value to said host, means for

connecting said security token to said host via a wired connection, and means for connecting said security token to said host via a wireless connection (e.g. paragraph [0028]).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. In particular, RSA newsletter published on November 1, 1999, Vol. 13 and issue 20. In the newsletter, RSA SedureID 3100 smart card is discussed. The RSA Secure ID 3100 can store two sets of 512- or 1,024 – bit RSA public and private cryptography keys, an RSA SecureID seed record, two digital certificates. Also, in the newsletter, Aladdin will integrate its eToken authentication solution with CyberTrust's PKI digital certificates. Therefore, Aladdin is able to offer a more customizable solution to the customers in the form of eToken. Applicant is **strongly urged** to review this reference in response to the current office action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

2 March 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100